Operations Security (OPSEC) Checklist For Publicly Accessible Army Websites (v 5.0):

Name:	Date/Time of Review:
Organization Reviewed:	Primary IP Address/URL:

Issue/Concern:	Yes	No	Notes/Comments:
Management Controls (Note: 1): 1. Does the Website (WS) contain a clearly defined purpose statement that supports the mission of the DoD Component? 2. Are users of this WS provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service. 3. If applicable does this WS contain a Disclaimer for External Links notice, when a user request any site outside of the official DoD web information service (usually the .mil domain)? 4. Is this WS free of commercial sponsorship and advertising?			

DEPSECDEF Guidance (Note 2):
 	
1. Operational Information:
 	
   a. Does the WS contain any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities?
 	
   b. Does the WS reference any information that would reveal sensitive			

movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program? 2. Personal Information: Does the WS contain personal information in the following categories about U.S. citizens, DOD employees and military personnel: • Social Security Account Numbers? • Dates of Birth? • Home Addresses? • Home Telephone Numbers? • Names, Locations, or any other identifying information about family members of DOD employees or military personnel? 3. Technological Data (Note 3): Does the WS contain any technical data such as: • Weapon Schematics? • Weapon System Vulnerabilities? • Electronic Wire Diagrams? • Frequency Spectrum Data?			
OPSEC Considerations: **"Tip Off Indicators" (Note 4):** Does the WS contain relevant information in the following categories that might reveal an organizations plans and intentions? 1. Administrative: • Personnel Travel (personal and official business).			

• Attendance at planning conferences. • Commercial support contracts. 2. Operations, Plans, and Training: • Operational orders and plans. • Mission specific training. • Exercise and simulations activity. • Exercise, deployment or training schedules. • Unit relocation/deployment. • Inspection results, findings, deficiencies. • Unit vulnerabilities or weaknesses. 3. Communications: • RF emissions and associated documentation. • Changes in activity or communications patterns. • Use of Internet and/or e-mail by unit personnel (personal or official business). • Availability of secure communications. • Hypertext links with other agencies or units. • Family support plans. • Bulletin board/messages between soldiers and family members. 4. Logistics/Maintenance: • Supply and equipment orders/deliveries. • Transportation plans. • Mapping, imagery and special documentation support. • Maintenance and logistics requirements. • Receipt or installation of special equipment.			

Key Word Search: Using the following "key words" conduct a search using the search tool. As a result of this search conduct a random screen of any documents found: • Deployment Schedules • Exercise Plans • Contingency Plans • Training Schedules • Inspection results, findings, deficiencies • Biographies • Family Support Activities • Phone Directories, Lists			

-NOTES PAGE-

Note 1: Management Controls are contained in the policy published by the Office of the Secretary of Defense, titled: <u>Establishing and Maintaining A Publicly Accessible Department Of Defense Web Information Service</u>, 9 January 1998.

Note 2: These elements were pulled directly from the DEPSECDEF memo, Information Vulnerability and the World Wide Web, dated, 24 Sept 98.

Note 3: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958.

Note 4: "Tip-off" indicators are pulled directly from AR 530-1, <u>Operations Security (OPSEC) regulation</u>, dated 3 Mar 95. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows him to pay closer attention and to task additional collection assets.

By necessity this list is generic in nature. There are many other indictors possible for the wide range of military operations and activities. While this list is rather large—when placed in the context of a commands **pre-established** critical information, this list may then be applied with a greater level of accuracy. This checklist is not a panacea for complete organizational OPSEC program. If an organization has not invested the effort to analyze it's own critical information, then this list my only tend to exacerbate the problem.

Within the context of information assurance, the World Wide Web should not be treated any differently from any other potential vulnerability. Security of information on publicly accessible web sites must be viewed in the context of an organization's overall OPSEC posture.